UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/737,389	12/16/2003	En-Yi Liao	10033.000400	5362

31894 7590 12/23/2005

OKAMOTO & BENEDICTO, LLP
P.O. BOX 641330
SAN JOSE, CA 95164

EXAMINER	
SERRAO, RANODHI N	
ART UNIT	**PAPER NUMBER**
2141	

DATE MAILED: 12/23/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/737,389	LIAO, EN-YI	
	Examiner	Art Unit	
	Ranodhi Serrao	2141	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 November 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed on 21 November 2005 have been fully considered but they are not persuasive.

2. Applicant argued that in Chen, the sender computer is not provided the location information of the authentication server instead of that of the receiving computer. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., the sender computer is not provided the location information of the authentication server instead of that of the receiving computer) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

3. Applicant furthermore argued that in Chen, data to be transferred between peer computers do not pass through the "interception node" or any node on the network whose location information has been substituted for that of the destination computer. The examiner points to col. 13, lines 26-30, wherein Chen describes an interception node. And col. 11, lines 24-49 states, "...the invention provides for the function calls establishing the communications to be intercepted and the initialization procedure routed through channel 61 to the authentication server 23." Moreover when the authentication server sends the data packet to the destination computer, the data packet itself consists of headers that contain source and destination addresses.

Therefore, the second peer node is provided with the location information of an interception node which is the authentication server.

4. The applicant also argued that Yeager fails to teach "the presence modifier being configured to provide to a second peer node a location information of an interception node instead of the location information of the first peer node in response to a detection of the publication." The examiner points to paragraphs 324 and 325, wherein the query handler serves the function of an interception node. Moreover, Yeager teaches publication of addresses and authentication or authorization services. And since the data packets themselves consist of headers containing source and destination addresses, the second peer node is provided with location information of the query handler or interception node instead of the location information of the first peer node.

5. In conclusion, the prior arts of record teach the invention as claimed, and the examiner reaffirms the rejections. See below.

Claim Rejections - 35 USC § 102

6. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

7. Claims 1-5, 7-11, 13, and 14 are rejected under 35 U.S.C. 102(b) as being anticipated by Chen et al. (6,061,796) (hereinafter referred to as Chen).

8. As per claim 1, Chen teaches a method of transferring data in a peer-to-peer computer network that includes a first peer node and a second peer node (col. 9, line 60-col. 10, line 11), the method comprising: providing the second peer node a location

information of an interception node instead of a location information of the first peer node in a data transfer between the first peer node and the second peer node; establishing a communication channel between the interception node and the second peer node (col. 11, lines 24-49); receiving the data in the interception node; and processing the data in the interception node (col. 9, lines 42-59).

9. As per claim 2, Chen teaches a method wherein the data are received by the interception node from the second peer node (col. 13, lines 17-25).

10. As per claim 3, Chen teaches a method further comprising: establishing a communication channel between the interception node and the first peer node; and wherein the data are received by the interception node from the first peer node (col. 4, lines 17-27).

11. As per claim 4, Chen teaches a method wherein the data comprise a file (col. 7, lines 25-35).

12. As per claim 5, Chen teaches a method wherein the location information of the first peer node comprises an IP address and a port number (col. 3, lines 16-29).

13. As per claim 7, Chen teaches a method wherein processing the data in the interception node comprises filtering the content of the data (col. 9, lines 42-59).

14. As per claim 8, Chen teaches a method further comprising: transferring the data from the interception node to the second peer node after the data have been processed in the interception node (col. 10, lines 37-58).

15. As per claim 9, Chen teaches a method further comprising: transferring the data from the interception node to the first peer node after the data have been processed in the interception node (col. 11, lines 24-49).

16. As per claim 10, Chen teaches a method of transferring a file in a peer-to-peer computer network, the method comprising: redirecting the file from a first peer node to an interception node, the file being originally intended to be transferred directly from the first peer node to a second peer node, the first peer node and the second peer node being computers in the peer-to-peer computer network (col. 6, line 66-col. 7, line 15); processing the file in the interception node (col. 9, lines 42-59); and transferring the file from the interception node to the second peer node (col. 10, lines 37-58).

17. As per claim 11, Chen teaches a method wherein the peer-to-peer computer network includes the Internet (col. 7, lines 25-34).

18. As per claim 13, Chen teaches a method wherein processing the file in the interception node comprises filtering a content of the file (col. 9, lines 42-59).

19. As per claim 14, Chen teaches a method wherein redirecting the file comprises: informing the second peer node that an address of the first peer node is that of the interception node (col. 12, lines 11-32).

20. Claims 16 and 19 rejected under 35 U.S.C. 102(e) as being anticipated by Yeager et al. (2003/0028585).

21. As per claim 16, Yeager et al. teaches a system for transferring data in a peer-to-peer network, the system comprising: a presence modifier configured to detect a

publication of a location information of a first peer node (paragraph 0162), the presence modifier being configured to provide to a second peer node a location information of an interception node instead of the location information of the first peer node in response to a detection of the publication (paragraph 0173), the first peer node and the second peer node being computers in the peer-to-peer computer network (paragraph 0013).

22. As per claim 19, Yeager et al. teaches a system wherein the location information of the first peer node comprises an IP address and a port number (paragraph 0315).

Claim Rejections - 35 USC § 103

23. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

24. Claims 6, and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chen et al. (6,061,796) as applied to claims 6 and 10 above, and further in view of Joiner et al. (6,789,117).

25. As per claim 6, Chen et al. teaches the mentioned limitations of claim 1 above but fails to teach a method wherein processing the data in the interception node comprises scanning the data for computer viruses. However, Joiner et al. teaches a method wherein processing the data in the interception node comprises scanning the data for computer viruses (see Joiner et al., col. 13, line 65-col. 14, line 4). It would have been obvious to one having ordinary skill in the art at the time of the invention to modify Chen et al. to a method wherein processing the data in the interception node comprises

scanning the data for computer viruses in order to scan network traffic and the detect intrusion in the network (see Joiner et al., col. 56-64).

26. As per claim 12, Chen et al. teaches the mentioned limitations of claim 10 above but fails to teach a method wherein processing the file in the interception node comprises scanning the file for viruses. However, Joiner et al. teaches a method wherein processing the file in the interception node comprises scanning the file for viruses (see Joiner et al., col. 13, line 65-col. 14, line 4). It would have been obvious to one having ordinary skill in the art at the time of the invention to modify Chen et al. to a method wherein processing the file in the interception node comprises scanning the file for viruses in order to scan network traffic and the detect intrusion in the network (see Joiner et al., col. 56-64).

27. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Chen et al. (6,061,796) as applied to claim 10 above, and further in view of Yeager et al. (2003/0028585). Chen et al. teaches the mentioned limitations of claim 10 above and a method of transferring the file from the interception node to the second peer node (see Chen et al., col. 11, lines 24-49). But fails to teach a method wherein transferring the file from the interception node to the second peer node comprises: querying a P2P server for location information of peer nodes involved in a transfer of the file; based on a response from the P2P server, identifying the second peer node as a node involved in the transfer of the file from the first peer node. However, Yeager et al. teaches a method wherein transferring the file from the interception node to the second peer node

comprises: querying a P2P server for location information of peer nodes involved in a transfer of the file (see Yeager et al., paragraph 0324); based on a response from the P2P server, identifying the second peer node as a node involved in the transfer of the file from the first peer node (see Yeager et al, paragraphs 0201-0202). It would have been obvious to one having ordinary skill in the art at the time of the invention to modify Chen et al. to a method wherein transferring the file from the interception node to the second peer node comprises: querying a P2P server for location information of peer nodes involved in a transfer of the file; based on a response from the P2P server, identifying the second peer node as a node involved in the transfer of the file from the first peer node in order to implement trust relationships between and among peers and to implement trust relationships between peers and content and data (see Yeager et al., paragraph 0014).

28. Claims 17, 18 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yeager et al. (2003/0028585) as applied to claim 16 above, and further in view of Joiner et al. (6,789,117).

29. As per claim 17, Yeager et al. teaches the mentioned limitations of claim 16 above but fails to teach a system further comprising: a data scanner in the interception node, the data scanner being configured to scan data passing through the interception node. However Joiner et al. teaches a system further comprising: a data scanner in the interception node, the data scanner being configured to scan data passing through the interception node (see Joiner et al., col. 13, line 65-col. 14, line 4). It would have been

obvious to one having ordinary skill in the art at the time of the invention to modify Yeager et al. to a system further comprising: a data scanner in the interception node, the data scanner being configured to scan data passing through the interception node in order to in order to scan network traffic and the detect intrusion in the network (see Joiner et al., col. 56-64).

30. As per claim 18, Yeager et al. teaches the mentioned limitations of claim 16 above but fails to teach a system wherein the interception node comprises a computer that is separate from a P2P server. However, Joiner et al. teaches a system wherein the interception node comprises a computer that is separate from a P2P server (see Joiner et al., col. 11, lines 42-53). It would have been obvious to one having ordinary skill in the art at the time of the invention to modify Yeager et al. to a system wherein the interception node comprises a computer that is separate from a P2P server in order to capture data being transmitted on a network (see Joiner et al., col. 1, lines 16-25).

31. As per claim 20, Yeager et al. teaches the mentioned limitations of claims 16 and 17 above but fails to teach a system wherein the data scanner is configured to scan the data for computer viruses. However, Joiner et al. teaches a system wherein the data scanner is configured to scan the data for computer viruses (see Joiner et al., col. 13, line 65-col. 14, line 4). It would have been obvious to one having ordinary skill in the art at the time of the invention to modify Yeager et al. to a system wherein the data scanner is configured to scan the data for computer viruses in order to in order to scan network traffic and the detect intrusion in the network (see Joiner et al., col. 56-64).

32. Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Yeager et al. (2003/0028585) as applied to claim 16 above, and further in view of Chen et al. (6,061,796). As per claim 21, Yeager et al. teaches the mentioned limitations of claim 16 above but fails to teach a system further comprising: a transfer manager in the interception node, the transfer manager being configured to obtain session information from the presence modifier. However, Chen et al. teaches a system further comprising: a transfer manager in the interception node, the transfer manager being configured to obtain session information from the presence modifier (col. 9, lines 1-10). It would have been obvious to one having ordinary skill in the art at the time of the invention to modify Yeager et al. to a system further comprising: a transfer manager in the interception node, the transfer manager being configured to obtain session information from the presence modifier in order to mutually authenticate users with respect to the server (see Chen et al., col. 4, lines 17-27).

33. Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Chen et al. (6,061,796) and Joiner et al. (6,789,117). Chen et al. teaches a method of transferring a file in a peer-to-peer computer network, the method comprising: transferring the file from a first peer node to an interception node, the file being originally intended to be transferred directly from the first peer node to a second peer node, the first peer node and the second peer node being computers in the peer-to-peer computer network (see Chen et al., col. 6, line 66-col. 7, line 15); and transferring the file from the interception node to the second peer node (see Chen et al., col. 10, lines 37-58). But

fails to teach a method of scanning the file for viruses in the interception node. However, Joiner et al. teaches a method of scanning the file for viruses in the interception node (see Joiner et al., col. 13, line 65-col. 14, line 4). It would have been obvious to one having ordinary skill in the art at the time of the invention to modify Chen et al. to a method of scanning the file for viruses in the interception node in order to scan network traffic and the detect intrusion in the network (see Joiner et al., col. 56-64).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ranodhi Serrao whose telephone number is (571)272-7967. The examiner can normally be reached on 8:00-4:30pm, M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Rupal Dharia can be reached on (571)272-3880. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

RUPAL DHARIA
SUPERVISORY PATENT EXAMINER